Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 8 June 2004 Meeting

GSA; 1800 F Street; Room 5141B; Washington, DC

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Approval Vote on Minutes from 11 May 2004
3) Status of Email Votes Since Last FPKIPA Meeting
4) New Working Group Recommendation
5) Federal Identity Credentialing Committee (FICC) Report
6) FPKI Certificate Policy Working Group (FPKI CPWG) Report
7) FBCA Operational Authority (FBCA OA) Report
8) Other Topics
9) Next Meeting Plans / Meeting Adjourned

B. VOTING MEMBER ATTENDANCE LIST

1) Department of the Treasury – Michelle Moldenhauer
2) Department of Commerce – Proxy by Tim Polk, NIST
3) Department of Justice – Proxy by Marty Burkhouse
4) Department of Defense – Proxy by Dave Hanko
5) General Services Administration – David Temoshok
6) Office of Management & Budget – Jeanette Thornton
7) National Aeronautics and Space Administration – Tice DeYoung
8) National Finance Center – Absent

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes:
Ms. Michelle Moldenhauer, Chair of the FPKIPA, called the meeting to order at 9:40 a.m. with attendee introductions.

Regarding the 11 May 2004 FPKIPA meeting minutes, only editorial comments were mentioned and later shared with IATAC after the meeting. Here is the voting record:

Approval vote for 11 May 2004 FPKIPA Meeting Minutes			
Voting members	**Vote (Motion – Justice; 2nd – DoD)**		
	Yes	**No**	**Abstain**
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice	X		
Dept of Defense	X		
GSA	X		
OMB (proxy by FPKIPA Chair)	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting:
There were no email votes conducted since the last FPKIPA meeting on 11 May 2004.

Agenda Item 4

New Working Group Recommendation:
Dr. Tice DeYoung, NASA, initiated this agenda item and distributed the discussion points in a PowerPoint presentation, entitled “Filling the Void” (Appendix A), via email to the FPKIPA mail list prior to this meeting.

The primary purpose of this discussion was to propose the establishment of a new working group to fill a perceived void of a working group forum between the existing high-level working groups - the FPKIPA (administrative) / CPWG (policy) and the low-level FBCA TWG (technical). Technical and business issues have been brought up for discussion at recent FPKIPA meeting but only because there is not a forum suitable for in-depth discussions on issues that affect the present and future of the FPKI. Dr. DeYoung suggested that this be an ad hoc working group, meeting on an “as needed basis”. He expects that the near-term actions of this group would be to discuss and recommend actions to the FPKIPA to address problems with current FBCA OA operations with cross-certification members.

OMB doesn’t want another FPKI working group established, especially if it will attract the same personnel that attend other FPKI working groups, unless it can be justified with an adequate charter, scope, deliverables, and membership comprised of implementers, not managers, to insure more of an action oriented working group. The opinion of most of the other attendees was that the FPKIPA charter allows for the establishment of other working groups to support perceived functions or topics in support of the overall FPKI mission, without having their own charter or needing any other approval for existence than the FPKIPA.

Someone raised the possibility of the technical topics being handled by the Path Discovery & Validation Working Group (PD-VAL). However, that idea was not seen as a viable possibility.

Similarly, the FPKI TWG, led by Bill Burr, NIST, was also recommended as a possible forum for these FPKI technical discussions. There was some consensus among the attendees that this idea may have some viability, but it would have to be discussed with Mr. Burr.

Mr. Dave Hanko, DoD, stated that the DoD PKI Business Working Group (BWG) handles business issues that impact the DoD PKI and suggested that the FPKI implement a similar working group to facilitate the discussion and effective handling of business issues. Ms. Michelle Moldenhauer, FPKIPA Chair, liked this concept, especially with the expected increase in business issues facing the FPKI with the advent of active shared service providers, etc.

ACTION (081): Dr. Tice DeYoung, NASA, will brief the status of the establishment of a new FPKI working group for technical/business issues at the 13 July FPKIPA meeting.

Agenda Item 5

Federal Identity Credentialing Committee (FICC) Report:
Mr. Brant Petrick, FICC, speaking on behalf of Ms. Judith Spencer, FICC Chair, reported the following items:

The Shared Service Providers (SSP) Subcommittee plans on having a Certified Providers List (CPL) for PKI Service Providers populated and posted to the Federal Identity Credentialing Committee (FICC) web site on June 30th. So far, there have been three Operational Capabilities Demonstration (OCD) tests scheduled for SSP candidates the week of June 14th.

The next FICC meeting is scheduled for July 7th. At this meeting, the primary discussion will be the Identity Assurance Working Group (IAWG) policy recommendations to the FICC for the minimum documents and procedures required for Federal agencies to issue a smart card identification badge.

The Office of Management and Budget (OMB) will be issuing a memorandum in the near future stating that Federal agencies who want to procure PKI services and smart cards must comply with the FICC approved Common PKI Policy and the FICC approved Smart Card Guidance document.

Agenda Item 6

FPKI Certificate Policy Working Group (CPWG) Report:
The following 4 things were on the agenda and covered by the CPWG Chair, Mr. Tim Polk, during this portion of the meeting:

1) Non-US Citizenship recommendation – None of the attendees knew the original source of why the FBCA CP required all CA operators to be US Citizens. But since non-US PKIs (such as Canada and possibly Australia) are now going through the process of cross-certification with the FBCA, it was stated and now understood by all attendees that this requirement cannot be required of non-US Entity CAs in the policy mapping. However, since this has been a long-standing requirement of cross-certification with the FBCA, there shouldn't be any reduction in this requirement for US Entity CAs. If a US Entity applicant PKIs wants to cross-certify with the FBCA or be an SSP, then they should be aware of this requirement and have CA trusted roles with US Citizenship.

   Since the US Citizenship requirement for CA operators is already part of the FBCA CP, there is no need to vote on this issue.

2) Common Policy Change Proposal, 2004-01 – Mr. Polk explained the recommended editorial changes to the Common Policy contained in this change proposal. The change proposal had numerous typos, which made it difficult to read and understand what was part of the change proposal. The attendees decided they wanted to see an updated version of this change proposal, before voting on it.

ACTION (082): Mr. Tim Polk, NIST, will distribute an updated version of the Common Policy Change Proposal, 2004-01, and request an electronic vote before the next FPKIPA meeting.

3) Department of Homeland Security (DHS) Mapping Report – this mapping report was unanimously approved by the FPKIPA members, per the following voting record:

Approval vote for Department of Homeland Security (DHS) Policy Mapping			
Voting members	**Vote (Motion – Justice; 2nd – Commerce)**		
	Yes	**No**	**Abstain**
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice	X		
Dept of Defense	X		
GSA	X		
OMB	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

ACTION (083): IATAC will provide the DHS primary POCs and their contact information to Jeanette Thornton, OMB.

4) Department of Labor (DoL) Mapping Report – this mapping report was unanimously approved by the FPKIPA members, per the following voting record:

Approval vote for Department of Labor (DoL) Policy Mapping			
Voting members	**Vote (Motion – NASA; 2nd – Justice)**		
	Yes	**No**	**Abstain**
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice	X		
Dept of Defense	X		
GSA	X		
OMB	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Mr. Polk also informed the attendees of the outcome of the 26 May joint FPKI CPWG / DoD PKI CPMWG meeting. The purpose of that meeting was to discuss the mapping performed by IATAC of the DoD CP compared to the FBCA CP, both in the new RFC 3647 format. Both the FPKI and the DoD PKI representatives left the meeting with some areas of their respective CPs to review and modify to make the CPs comparable to each other.

Agenda Item 7

FBCA Operational Authority (OA) Report:

Status of FBCA Certification & Accreditation (C&A)
Mr. Darron Tate reviewed the status of the FBCA Certification & Accreditation, stating the following highlights:

- The FBCA OA is undergoing C&A retesting with KPMG today. This testing primarily includes residual issue resolution.
- The FBCA OA is getting documents ready for the DAA by 22 June and moving forward with plans and arrangements for a full ATO, with a target completion date of early July 2004.
- The E-Governance Policy for Assurance Levels 1 & 2 (addressing server certificates) is needed. CP/CPS Compliance Audit of the FBCA must be done by the start of FY05 so this policy is needed fairly soon. CPWG already has the action (Action #075) to develop this E-Governance Policy and it would be better to have it done by the end of July, to make sure it receives all the right approvals, rather than wait until closer to the start of FY2005. Ms. Cheryl Jenkins stated that she has written the Standard Operating Procedure (SOP) document for the FBCA OA to issue certificates using Level 1 and Level 2 authentication. Since this SOP is just for Level 1 and Level 2, the FPKIPA should review and give it an approval.

Status of FBCA/Applicant Cross-Certification Technical Testing:
The LDAP Testing Matrix is currently being developed and will be available on the website in early July 2004.

Technical testing started with Department of Homeland Security (DHS) four days ago. However, DHS doesn't currently have a border directory so the directory testing cannot be completed until that is established at DHS.

The FBCA OA passed out the "Analysis of Entity Certification Authority Demonstrations, Department of Labor, dated 7 June 2004" that documents the findings of the DoL Technical Testing. The FPKIPA voted to approve the DoL Technical Testing, per the following voting record:

Approval vote for Department of Labor Technical Testing			
Voting members	**Vote (Motion – Commerce; 2nd – NASA)**		
	Yes	**No**	**Abstain**
Dept of the Treasury	X		
Dept of Commerce	X		
Dept of Justice (proxy by FPKIPA Chair)	X		
Dept of Defense	X		
GSA	X		

OMB	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Status of CA Testing:

The following technical issues were described by Mr. Andrew Lins, Mitretek, and discussed during this meeting:

1) LDAP Directory requirements for the FBCA CP --- The FBCA OA reduced some of the LDAP directory requirements that are part of the interoperability testing. Based on the FBCA OA implementation, it is not clear which LDAP directory requirements should be retained and why, mostly because the original source of the requirements is unknown. The FBCA OA thinks the LDAP directory requirements that are used in the technical testing should be included in the FBCA CP – is this agreeable to the FPKIPA? The attendees believe that there may possibly be some that should be incorporated into the FBCA CP, but they would have to review them. If they are technical requirements, they should remain in the technical testing and not be added to the FBCA CP.

2) Revocation reason --- the FBCA OA asked if a certificate reason code may be changed after a certificate has been revoked. The FPKIPA wasn't sure why this would need to be done, but Treasury took an action to look at their CP and see if it mentions this requirement or if this practice is allowed in their implementation.

ACTION (084): Department of the Treasury will review their CP and determine if it allows the practice of changing the reason code in a certificate after that particular certificate has been revoked.

3) FBCA Directory --- There are currently two directories behind the firewall. One is public access and one is for chaining port access only. The FBCA OA is concerned that about Denial Of Service (DOS) attacks on the public access directory. What are the alternatives, if the FBCA OA doesn't want to be open to DOS attacks? The FPKIPA believes the directory should remain as public access, but appreciated bringing this topic up for discussion.

4) Inconsistency between FBCA OA operations and FBCA CP requirements for CRLs --- One of the KPMG findings during C&A testing was Section 6.7.1, Paragraph 1 of the FBCA CP describes an out-of-band issuance method for CRLs. However, in reality, the FBCA OA operates with automatic publishing of CRLs. The FBCA OA requested the immediate drafting of a FBCA CP Change Proposal and vote among the FPKIPA members at this meeting, since without changing the FBCA CP regarding this issue makes the FBCA OA operations non-compliant and unable to pass the current C&A testing. Mr. Polk drafted a FBCA CP change proposal and the FPKIPA members voted on it per the following voting record:

Approval vote for FBCA CP Change Proposal, 2004-01			
Voting members	**Vote (Motion – NASA; 2nd – Treasury)**		
	Yes	**No**	**Abstain**
Dept of the Treasury	X		
Dept of Commerce	X		

Dept of Justice (proxy by FPKIPA Chair)	X		
Dept of Defense (proxy by FPKIPA Chair)	X		
GSA	X		
OMB (proxy by FPKIPA Chair)	X		
NASA	X		
NFC (proxy by FPKIPA Chair)	X		

Agenda Item 8

Other Topics:

Action Item Review
No changes to the Action Item list were necessary at this time.

Compliance Audit Report
Department of the Treasury submitted their annual compliance audit report for their Root CA to the FPKIPA.

Agenda Item 9

Next Meeting Plans / Meeting Adjourned:
The next FPKI PA Meeting is scheduled for 13 July 2004 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 5141B, Washington, DC.

The meeting adjourned at 11:30 a.m.

D. LIST OF ATTENDEES

NAME	Email	Telephone	Organization
Alterman, Peter	altermap@mail.nih.gov	301.252.8846	HHS
Burkhouse, Marty	martin.t.burkhouse@usdoj.gov	202.616.4574	DoJ
DeYoung, Tice	tdeyoung@hq.nasa.gov	202.358.2154	NASA
Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681	eValid8
Faut, Nathan	nfaut@educause.edu	301.335.2656	HEBCA
Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900	DoD
Lentz, Mark	lentz_mark@bah.com	410.684.6520	IATAC
Lins, Andrew	andrew.lins@mitretek.org	703.610.1786	MTS
Moldenhauer, Michelle	michelle.moldenhauer@do.treas.gov	202.622.1110	Treasury
Petrick, Brant	brant.petrick@gsa.gov	202.208.4673	FICC
Polk, Tim	tim.polk@nist.gov	301.975.3348	NIST
Stipisic, Dario	dario.stipisic@bearingpoint.com	703.519.2534	BearingPoint
Tate, Darron	darron.tate@mitretek.org	703.610.1905	MTS
Temoshok, David	david.temoshok@gsa.gov	202.208.7655	GSA
Thornton, Jeanette	jeanette_i._thornton@omb.eop.gov	202.395.3562	OMB

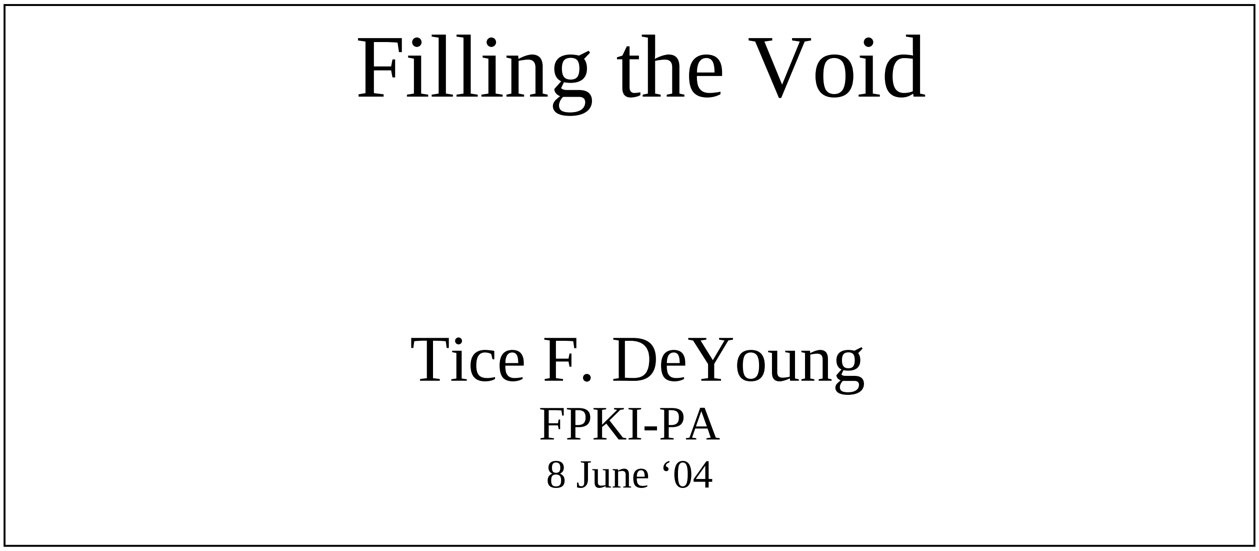
E. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
004	Define the audit criteria (Web Methods, SAS70, PAG) that will be used to conduct C&A sessions for the FBCA and FBCA OA. 14 January 2003 – This delta report of what is covered by each C&A technique has been deferred until the completion of the FBCA Criteria and Methodology documents.	Tice DeYoung, NASA	08 April 2002 Updated – 14 Jan 2003 Updated – 13 May 2003	13 Jan 2004 FPKIPA meeting	**Open –** reassigned to GSA/FTS, Cheryl Jenkins (as of 14 Jan 2003) and Tice DeYoung (13 May 2003)
043	Establish policy to reflect the changing interoperability needs of the multiple membrane members, and forward requested changes to Mr. John Cornell for review before sending out to the working group members.	Tim Polk, NIST	13 May 2003	13 Jan 2004 FPKIPA meeting	**Open**
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	**Open**
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
061	Incorporate the new FBCA CP Change Proposals (2003-01 through 2003-05) into the FBCA CP, dated 10 September 2002, and forward the resulting FBCA CP to the FPKIPA webmaster for posting to the Federal PKI web sites.	IATAC	9 Sept 2003	31 Dec 2003	**Open**
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	**Open**
075	Develop, approve, and forward to the FPKIPA an E-Governance Certificate Policy for Assurance Levels 1 & 2 by 1 October 2004.	FBCA CPWG	9 Mar 2004	1 Oct 2004	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
076	Check the accuracy of the dates and contact information in the Microsoft agreement (Action Item #68) and then distribute it to the FPKIPA and the CPWG.	FBCA OA	9 Mar 2004	13 Apr 2004 FPKIPA meeting	**Open**
078	Present a briefing at the 10 August FPKIPA meeting on the status of their PKI interoperability requirements and guidance research.	DoD PAT	11 May 2004	10 Aug 2004 FPKIPA meeting	**Open**
079	Develop a recommendation for how to indicate non-US citizenship in an X.509 certificate and present it at the 8 June FPKIPA meeting for consideration.	NIST	11 May 2004	8 June 2004 FPKIPA meeting	**Closed, 8 June FPKIPA meeting**
080	Provide the Level 1 and Level 2 SOP to IATAC and IATAC will distribute to the CPWG for review and approval vote.	FBCA OA	11 May 2004	8 June 2004 FPKIPA meeting	**Closed, 9 June email vote**
081	Brief the status of the establishment of a new FPKI working group for technical/business issues at the 13 July FPKIPA meeting.	Dr. Tice DeYoung, NASA	8 June 2004	13 July 2004 FPKIPA meeting	**Open**
082	Distribute an updated version of the Common Policy Change Proposal, 2004-01, and request an electronic vote before the next FPKIPA meeting.	Tim Polk, NIST	8 June 2004	13 July 2004 FPKIPA meeting	**Closed, 9 June email vote**
083	Provide the DHS primary POCs and their contact information to Jeanette Thornton, OMB.	IATAC	8 June 2004	22 June 2004	**Closed, 17 June email**
084	Review the Treasury CP and determine if it allows the practice of changing the reason code in a certificate after that particular certificate has been revoked.	Dept of the Treasury	8 June 2004	10 August 2004 FPKIPA meeting	**Open**

Appendix A:

PowerPoint Presentation from Agenda Item 4 – New Working Group Recommendation

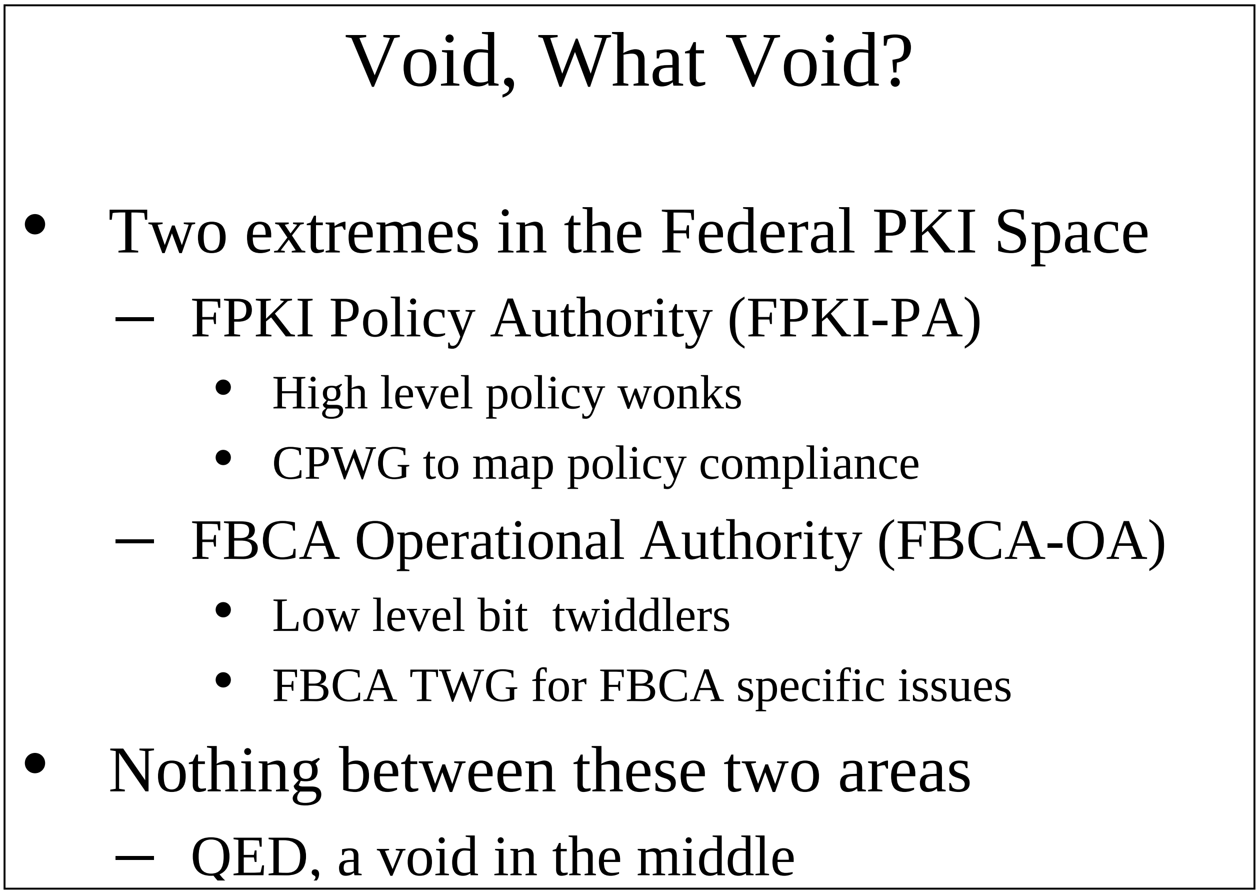


Filling the Void

Tice F. DeYoung

FPKI-PA

8 June ‘04



Void, What Void?

- Two extremes in the Federal PKI Space
  - FPKI Policy Authority (FPKI-PA)
    - High level policy wonks
    - CPWG to map policy compliance
  - FBCA Operational Authority (FBCA-OA)
    - Low level bit twiddlers
    - FBCA TWG for FBCA specific issues
- Nothing between these two areas
  - QED, a void in the middle

How to Fill the Void

- Need an FPKI group that sits below the high level policy wonks and above the bit twiddlers
  - A group that will
    - Answer agencies questions about PKI
    - Discuss technical issues and future directions in FPKI
    - Host a FAQ list about PKI with answers and how to dos
  - A group that will act
    - As a mentor to other agencies
    - As an intelligent clearing house
  - A group that will tackle the inter-agency issues associated with public key infrastructure
    - Tries to solve the issue of public encryption keys for addressees outside their own agency
    - Looks at the issue of full path discovery and validation for every transaction

What Questions About PKI?

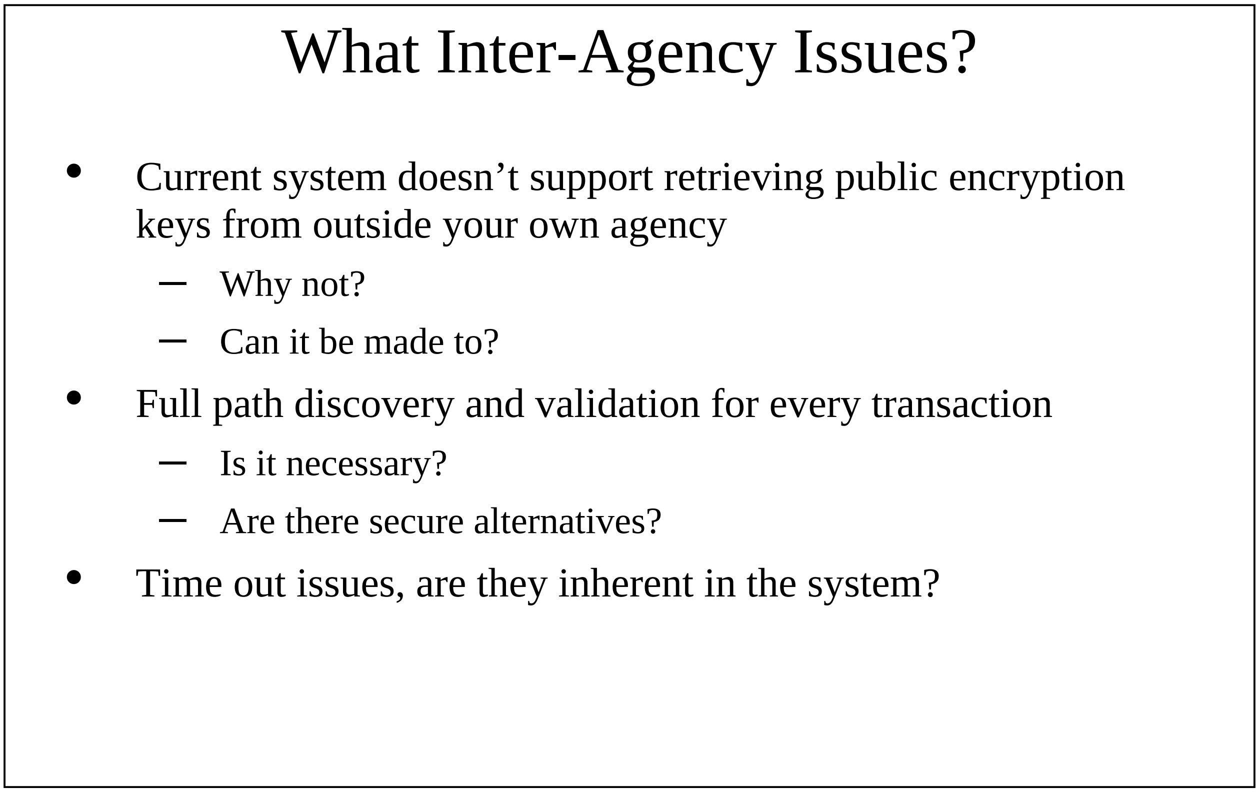
- How do they go about implementing PKI?
  - What is PKI and who are the vendors?
  - Do they do it themselves or outsource it to another US Government Agency or ACES vendor or a Shared Service Provider (SSP)?
    - If they outsource it, do they
      - archive the keys themselves or outsource it?
      - provide the Registration Authority or do they outsource the function?
      - participate in any of the management function or not?
    - If they want to do it themselves, can they justify it?
      - Specific reasons that they must maintain control of their PKI
      - Business case that in-house is more cost effective

Mentor and Clearinghouse, How?

- Provide a safe haven where they won’t feel foolish
  - A place where they will be welcomed as equals
  - A place where people don’t have ulterior motives (for the most part)
  - A place where they will get the help they need
- Provide a clearinghouse for PKI
  - Prevent re-inventing the PKI wheel, yet again
  - Share war stories
  - Share documents
  - Share ideas

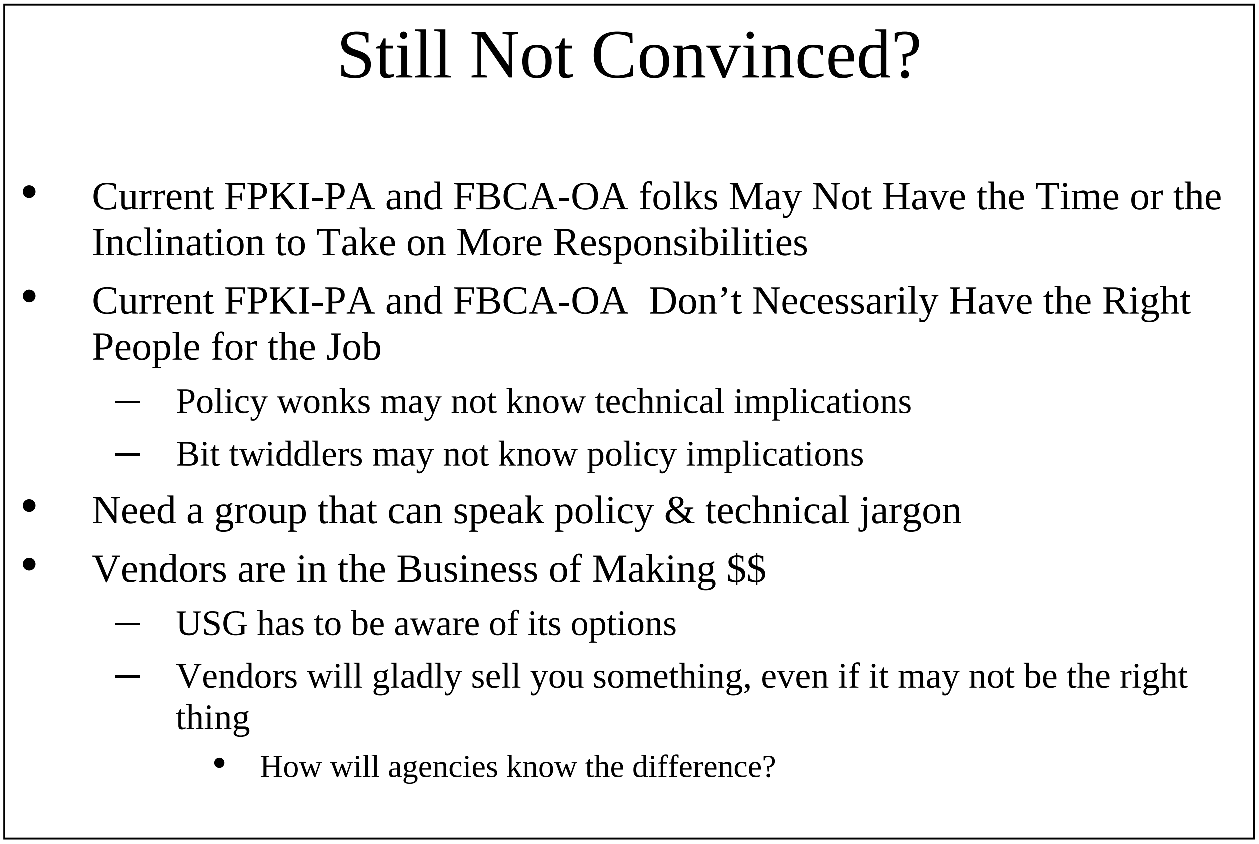
What FBCA Discussions?

- Technical issues
  - Should the FBCA expand beyond CRLs only?
    - OCSP SCVP
    - XKMS Others?
  - How do we solve the bridge to bridge to bridge problem?
    - Meta bridge? God like trust anchor?
    - Trusted bridge cloud or axle?
  - Should we look at new architectures for the FBCA?
  - Are there newer technologies that are better?
- Future Directions for FPKI



What Inter-Agency Issues?

- Current system doesn’t support retrieving public encryption keys from outside your own agency
  - Why not?
  - Can it be made to?
- Full path discovery and validation for every transaction
  - Is it necessary?
  - Are there secure alternatives?
- Time out issues, are they inherent in the system?



Still Not Convinced?

- Current FPKI-PA and FBCA-OA folks May Not Have the Time or the Inclination to Take on More Responsibilities
- Current FPKI-PA and FBCA-OA Don’t Necessarily Have the Right People for the Job
  - Policy wonks may not know technical implications
  - Bit twiddlers may not know policy implications
- Need a group that can speak policy & technical jargon
- Vendors are in the Business of Making $$
  - USG has to be aware of its options
  - Vendors will gladly sell you something, even if it may not be the right thing
    - How will agencies know the difference?

Where Will It Fit & How Will it Function?

- The FPKI AdHoc Working Group (FPKI-AHWG) will be a working group of the FPKI-PA.
  - – It will report to the FPKI-PA on technical & policy issues
    - It will advise the FPKI-PA on policy matters that have technical implications
    - It will advise the FBCA-OA on technical matters that may have policy implications
- The group will be comprised of USG agencies cross-certified with the FBCA
  - – Special technical and policy experts will be brought in as needed

Discussion

Questions, Comments, Slings & Arrows?